Acronis Privacy Expert Corporate

User's Guide

Acronis
Compute with confidence

www.acronis.com

Copyright © Acronis, Inc., 2000-2005. All rights reserved.

Windows is registered trademarks of Microsoft Corporation.

All other trademarks and copyrights referred to are the property of their respective owners.

Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of this work or derivative work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

DOCUMENTATION IS PROVIDED «AS IS» AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

END-USER LICENSE AGREEMENT

BY ACCEPTING, YOU (ORIGINAL PURCHASER) INDICATE YOUR ACCEPTANCE OF THESE TERMS. IF YOU DO NOT WISH TO ACCEPT THE PRODUCT UNDER THESE TERMS, YOU MAY CHOOSE NOT TO ACCEPT BY SELECTING "I decline..." AND NOT INSTALLING THE SOFTWARE.

The Acronis Privacy Expert Corporate (the software) is Copyright © Acronis, Inc., 2000-2005. All rights are reserved. The ORIGINAL PURCHASER is granted a LICENSE to use the software only, subject to the following restrictions and limitations.

1. The license is to the original purchaser only, and is not transferable without prior written permission from Acronis.
2. The original purchaser may use the software on a single computer owned or leased by the original purchaser. You may not use the software on more than one machine even if you own or lease all of them, without the written consent of Acronis.
3. The original purchaser may not engage in, nor permit third parties to engage in, any of the following:

A. Providing or permitting use of or disclosing the software to third parties.

B. Providing use of the software in a computer service business, network, timesharing or multiple user arrangement to users who are not individually licensed by Acronis.

C. Making alterations or copies of any kind in the software (except as specifically permitted above).

D. Attempting to un-assemble, de-compile or reverse engineer the software in any way.

E. Granting sublicenses, leases or other rights in the software to others.

F. Making copies or verbal or media translations of the users guide.

G. Making telecommunication data transmission of the software.

Acronis has the right to terminate this license if there is a violation of its terms or default by the original purchaser. Upon termination for any reason, all copies of the software must be immediately returned to Acronis, and the original purchaser shall be liable to Acronis for any and all damages suffered as a result of the violation or default.

ENTIRE RISK

THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE IS WITH YOU THE PURCHASER. ACRONIS DOES NOT WARRANT THAT THE SOFTWARE OR ITS FUNCTIONS WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE OR THAT ANY DEFECTS WILL BE CORRECTED. NO LIABILITY FOR CONSEQUENTIAL DAMAGES — IN NO EVENT SHALL ACRONIS OR ITS VENDORS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR THE LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF ACRONIS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Table of Contents

END-USER LICENSE AGREEMENT 3

INTRODUCTION 6

What is Acronis Privacy Expert Corporate? 6
Acronis Privacy Expert Corporate key features 6
Acronis Privacy Expert Corporate Architecture 7
Software use conditions 7
Technical support 8

CHAPTER 1. INSTALLING ACRONIS PRIVACY EXPERT CORPORATE COMPONENTS 9

1.1 System requirements 9
1.2 Supported operating systems 9
1.3 Setting up security parameters for Acronis Privacy Expert Corporate 9
1.3.1 Usernames and passwords 9
1.3.2 Firewall setup 10
1.4 License policy 10
1.5 Installing Acronis Privacy Expert Corporate components onto a current computer 10
1.6 Extracting Acronis Privacy Expert Corporate components 11
1.7 Using License Server Management Tool 11
1.8 Installing Acronis components onto remote machines 12
1.9 Recovering Acronis Privacy Expert Corporate 13
1.10 Removing Acronis Privacy Expert Corporate 13

CHAPTER 2. USING ACRONIS PRIVACY EXPERT CORPORATE MANAGEMENT CONSOLE 14

2.1 Getting started 14
2.2 Acronis Privacy Expert Corporate Management Console main window 14
2.3 Connecting to remote computer 15

CHAPTER 3. SPYWARE REMOVAL FROM NETWORK COMPUTERS 16

3.1 How spyware gets on user's PC 16
3.2 How to recognize spyware? 16
3.3 Spyware removal 17
3.3.1 Running Spyware Removal Wizard 17
3.3.2 Selecting remote computers for spyware removal 17
3.3.3 Selecting scanning mode 18
3.3.4 Spyware Removal Script 19
3.4 Scheduling spyware removal group tasks 19
3.4.1 Selecting remote computers 19
3.4.2 Selecting task and spyware scan mode 20
3.4.3 Scheduled tasks preferences 20
3.4.4 Entering user name and password 21
3.5 Quarantine 22
3.6 Using the Log 23

CHAPTER 4. USING ACRONIS SPYWARE SHIELD 25

4.1 Enabling Acronis Spyware Shield 25
4.2 Spyware Shield local settings 26
4.2.1 General options 26
4.2.2 Advanced options 27
4.2.3 Remembered events 27
4.2.4 Saving Spyware Shield settings 28

CHAPTER 5. SPYWARE DEFINITIONS UPDATES 29

Copyright © Acronis, Inc., 2000-2005

5.1 Product registration 29
5.2 Spyware database update 29
5.2.1 Running Spyware Definitions Updates Wizard 29
5.2.2 Selecting remote computers to update spyware definitions 30
5.2.3 Selecting update mode 30
5.2.4 Setting the schedule 31
5.2.5 Entering user name and password 32

CHAPTER 6. ACRONIS POP-UP BLOCKER 33

6.1 What are pop-ups? 33
6.2 Acronis Pop-up Blocker 33
6.3 Acronis Pop-up Blocker local options 33
6.3.1 Acronis Pop-up Blocker general settings 34
6.3.2 Last visited pages 34
6.3.3 Blocked URLs 34
6.3.4 White URLs 34
6.3.5 Black URLs 35

CHAPTER 7. OTHER OPERATIONS 36

7.1 Creating a bootable diskette or CD with Acronis Drive Cleanser 36
7.2 Data destruction with Acronis Drive Cleanser 36

APPENDIX A. SPYWARE THREATS GLOSSARY 38

Adware 38
Browser Helper Objects 38
Browser hijackers 38
Commercial keylogger 38
Dialers 38
Exploit/Security holes 39
Remote Administration 39
Sniffers 39
Spyware 39
Toolbars 39
Trojan Horses (Trojans) 39

Copyright © Acronis, Inc., 2000-2005

Introduction

What is Acronis Privacy Expert Corporate?

Spyware, a technology that aids crooks and others gather information about a person or organization without their knowledge, is becoming a huge threat to business networks. It can **leak valuable, confidential information about your organization** to outside entities and can ultimately slow down network performance, impacting your employees' productivity. IT managers recognize spyware's potential negative impact. According to a January 2005 survey, two thirds of IT managers think that spyware is the number one security **threat to their networks**.

Acronis has a solution to **ensure that spyware will not be a threat to your organization or corporate network**. The Acronis Privacy Expert Corporate is a comprehensive anti-spyware solution that **proactively protects** your organization from spyware programs that can expose confidential information and diminish PC performance.

Acronis Privacy Expert Corporate is **more than just an anti-spyware solution.** It also includes **value-added security tools** that ensure your **employee** data and **actions are secure**.

Acronis Privacy Expert Corporate key features

- **Remote deleting of spyware programs** from network computers to ensure that outside entities do not obtain access to internal/confidential data
    - Managing spyware tasks on networked computers from one central location
    - Scheduling spyware scans on all networked computers on a regular basis without user intervention
    - Smart scanning searches for spyware in the most likely locations, including system, user profile and temporary files folders, as well as in the system registry
    - Deep scanning searches all folders on the PC hard drive
    - Keylogging detection protects usernames and passwords from getting into outside hands
    - Quarantine feature enables the administrator to look through the list of the objects (files, registry keys etc.), deleted by spyware removal operations, and restore any of them, in the unlikely case it would be useful
- **Remote installation** of Acronis Privacy Expert Corporate components to network computers

 Copyright © Acronis, Inc., 2000-2005

- **Comprehensive Spyware Shield** prevents spyware from being installed to networked computers
    - Constantly monitors running processes and provides alerts due to any suspicious actions of programs, such as trying to change the Windows registry and to launch at startup
    - Prevents the changing of settings of ActiveX components
    - Prevents applications from making changes to Web browser settings, including home page, search page, etc. This ensures that employees go to the pages they select
- **Pop-up ad blocker** ensures that annoying pop-up ads do not interfere with Web browsing
- **Internet updates** service keeps spyware definitions up-to-date. Updates can be downloaded manually via a wizard or automatically downloaded as a scheduled task
- **Acronis knowledge base**, an online information resource, provides comprehensive details on topics such as where specific spyware threats come from, what has to be changed if one decides to remove spyware manually, and other useful information

Acronis Privacy Expert Corporate Architecture

Acronis Privacy Expert Corporate includes the following components:

1. Acronis Privacy Expert Corporate Management Console — helps you install and manage the Acronis Privacy Expert Corporate Agent on a remote machine; removes spyware threats on the remote computers, schedules spyware removal tasks, browses logs and more

2. Acronis Privacy Expert Corporate Agent — installs on a remote system to enable access from the Acronis Privacy Expert Corporate Management Console

3. Acronis Spyware Shield — installs on a remote computers and monitors it for suspicious applications and components

4. **Acronis Pop-up Blocker -** installs on a remote computers and blocks unwanted pop-up windows there

5. Acronis License Server allows you to manage your Acronis enterprise product licenses from a single location.

Software use conditions

The conditions for Acronis Privacy Expert Corporate software usage are described in the «License Agreement» (page 3 of this manual). A set of unique serial keys, supplied with the product, is the confirmation of the legal purchase and usage the suite.

Copyright © Acronis, Inc., 2000-2005

Under current legislation, the «License Agreement» is considered a contract between the user and software vendor. The contract is a legal document and its violation may result in legal action.

Illegal use and/or distribution of this software will be prosecuted

Technical support

Users of legally purchased and registered copies of Acronis Privacy Expert Corporate are entitled to free e-mail and fax technical support from Acronis. If you have installation or working problems that you cannot solve by yourself using this manual, please contact the technical support team. When e-mailing technical support, you must provide the software registration information.

For more information visit http://www.acronis.com/enterprise/support/

For product registration visit http://www.acronis.com/enterprise/registration/

Technical support e-mail address: support@acronis.com

Copyright © Acronis, Inc., 2000-2005

Chapter 1. Installing Acronis Privacy Expert Corporate components

1.1 System requirements

To take full advantage of Acronis Privacy Expert Corporate, you should have:

- a PC-compatible computer with a Pentium CPU or equivalent
- 64 MB RAM
- a floppy or a CD-RW drive
- a mouse (recommended)
- Microsoft Internet Explorer 4.0 or higher for correct Pop-up Blocker operation

1.2 Supported operating systems

Acronis Privacy Expert Corporate Management Console:

- MS Windows 98/Me
- MS NT 4.0 Workstation Service Pack 6 / 2000 Professional / XP Professional
- MS NT 4.0 Server Service Pack 6 / 2000 Server / 2000 Advanced Server, 2003 Server.

Acronis Privacy Expert Corporate Agent:

- MS Windows 98 / Me /
- MS Windows NT 4.0 Workstation SP 6 / 2000 Professional / XP Professional.

1.3 Setting up security parameters for Acronis Privacy Expert Corporate

1.3.1 Usernames and passwords

Acronis Privacy Expert Corporate fully supports all security standards used in Windows:

1. If a remote PC has Windows NT/2000/XP OS installed, the Acronis Privacy Expert Corporate Agent can be accessed according to the security policy set up in the local network. To have remote access to Acronis Privacy Expert Corporate Agent, the user must be a member of the **Administrators** group on this computer.

It is highly recommended that you create an administrator's account with the same username and password on all networked computers for remote access to the Acronis Privacy Expert Corporate Agent.

2. If a remote PC has Windows 98/Me installed without its own security system, you will need to provide a username and password during installation of the

Copyright © Acronis, Inc., 2000-2005

Acronis Privacy Expert Corporate Agent that will be used by Acronis Privacy Expert Corporate Management Console.

1.3.2 Firewall setup

Acronis Privacy Expert Corporate uses the following ports and IP addresses for remote operation:

- **SERVER (ACRONIS PRIVACY EXPERT CORPORATE AGENT) UDP PORT:** 9876
- **SERVER (ACRONIS PRIVACY EXPERT CORPORATE AGENT) TCP PORT:** 9876, IF BUSY CHOSE PORT AT RANDOM
- **CLIENT (ACRONIS PRIVACY EXPERT CORPORATE MANAGEMENT CONSOLE) UDP PORT:** 9877, IF BUSY CHOSE PORT AT RANDOM
- **IPV4 MULTICAST ADDRESS:** 239.255.219.45
- **IPV6 MULTICAST ADDRESS:** FF05::FAA5:741E

You might have to set the appropriate firewall access options. Options for the Windows Firewall, included in Windows XP Service Pack 2, are set automatically during Acronis Privacy Expert Corporate components installation. However, make sure that the option **File and Printer Sharing** in the **Control panel** → **Windows Firewall** → **Exceptions** is enabled on the remote computer before the remote operation starts.

1.4 License policy

Acronis Privacy Expert Corporate licensing is based on the number of workstations on which the **Acronis Privacy Expert Corporate Agent** is to be installed. The number of **Acronis Privacy Expert Corporate Management Console** or **Acronis License Server** installations is not counted.

To manage the corporate license information, you must install **Acronis License Server** and import the license data (serial keys) bundled with your Acronis Privacy Expert Corporate copy (see 1.7 “Using License Server Management Tool”). If you buy more licenses, import the additional serial keys as well.

Acronis License Server can import multiple serial numbers from a .txt file, saving you from time-taking procedure of typing in serial keys.

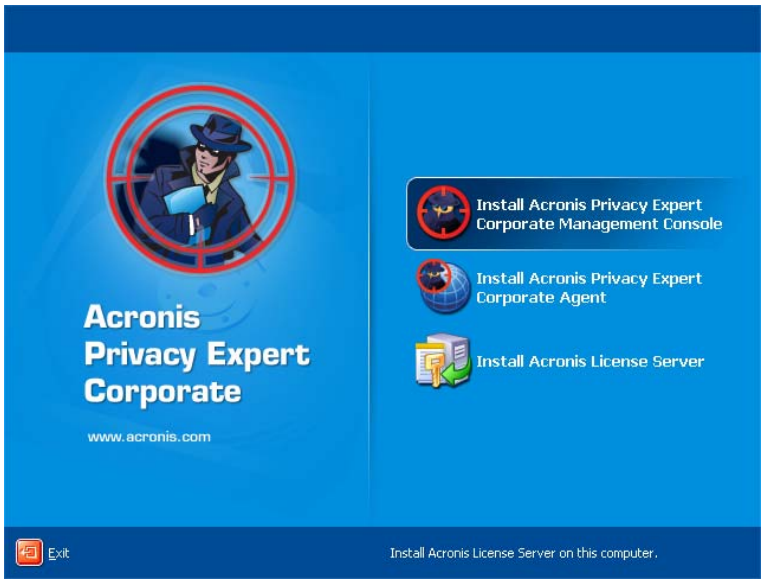
1.5 Installing Acronis Privacy Expert Corporate components onto a current computer

Run Acronis Privacy Expert Corporate setup file. In the Install Menu, select the component that you are going to install on a current PC: Acronis Privacy Expert Corporate Management Console, Acronis Privacy Expert Corporate Agent or Acronis License Server. Follow instructions shown in the installation wizard.

 Copyright © Acronis, Inc., 2000-2005

It is recommended that you install Acronis License Server first. You will not be able to install Acronis Privacy Expert Corporate Agent onto the current or remote computer until you import the serial key into Acronis License Server.

When the Specify License Server window appears, specify the License Server for license validation. It can be found automatically on the local network or specified manually (type in the DNS-name of the computer with Acronis License Server installed, or its IP-address).



Acronis Privacy Expert Corporate installation window

After installation is completed, you may be prompted to restart your computer.

1.6 Extracting Acronis Privacy Expert Corporate components

You may want to save setup (.msi) files for each Acronis Privacy Expert Corporate component separately on a local or network drive. Then you will be able to install the components in the command-line mode using msiexec.exe utility. It also will help to modify or recover the existing component installation.

To save a setup file:

- run the Acronis Privacy Expert Corporate setup file;
- in the Install Menu, right-click on the component name and select **Extract**;
- select location for setup file and click **Save**.

1.7 Using License Server Management Tool

Acronis License Server includes special command-line utility **LicenseServerCmdLine.exe** for managing license information. Using this tool, you can look through and add information on available licenses.

After Acronis License Server installation **LicenseServerCmdLine.exe** is located in the installation folder, e. g. C:\Program Files\Acronis\LicenseServer.

Copyright © Acronis, Inc., 2000-2005

LicenseServerCmdLine.exe uses the following syntax:

`LicenseServerCmdLine [option] [parameter1] [parameter2]`

LicenseServerCmdLine.exe supported options and usage:

`--list`

Displays the list of the License servers available in the local network.

`--status [server name or server IP-address]`

Displays specified License Server status.

`--import [server name] [serial key]`

Adds information about new license (new serial key). You can specify multiple serial numbers (space separated).

`--import-file [server name] [filename]`

Imports license serial keys from .txt file.

`--help`

Shows help information.

1.8 Installing Acronis components onto remote machines

Acronis Privacy Expert Corporate Management Console allows you to install Acronis components onto remote computers, connected to the corporate network.

Using the Acronis Privacy Expert Corporate Management Console, you can install remotely:

- Acronis Privacy Expert Corporate Agent
- Acronis Spyware Shield
- Acronis Pop-up Blocker
- Acronis License Server

To install any Acronis component to a remote machine, you will need administrator rights on the target machine.

You can remotely install Acronis components only onto machines working under Windows NT/2000/XP (including server versions). Windows 98/Me machines will require local installation of Acronis components.

If the remote PC runs under Windows XP, make sure the option **Use simple file sharing** in the **Control panel → Folder options → View** is disabled before the remote installation starts.

If the remote PC runs under Windows XP with Service Pack 2 installed, make sure that the option **File and Printer Sharing** in the **Control panel → Windows Firewall → Exceptions** is enabled before the remote installation starts.

To install Acronis components:

 Copyright © Acronis, Inc., 2000-2005

- Select the **Install Acronis components** button on the Toolbar or select **Tools → Install Acronis components** from the main menu
- Select the Acronis components you want to install (Acronis Privacy Expert Corporate Agent, Acronis Spyware Shield, Acronis Pop-up Blocker or Acronis License Server)
- In the next window, select the remote computers on which the Acronis components are to be installed
- If the Specify License Server window appears, specify the License Server for license validation. It can be found automatically on the local network or specified manually (type in the DNS-name of the computer with Acronis License Server installed, or its IP-address)
- The Acronis components then will be installed to the remote PCs you specified
- If you checked **Reboot the remote computer(s)** box during the component installation, the remote machines will reboot. Otherwise, you will see the corresponding message.

1.9 Recovering Acronis Privacy Expert Corporate

You can reinstall Acronis Privacy Expert Corporate components if nesessary. To do this, launch the installation program again.

The installer will determine that the component has already been installed to your PC and ask if you want to **Modify, Repair** or **Remove** it from the disk.

Select **Repair** Acronis Privacy Expert Corporate and click **Next**. All files will be copied to your hard disk again to restore the program.

To repair Acronis Privacy Expert Corporate components installed on remote computers, reinstall them as described in 1.8.

1.10 Removing Acronis Privacy Expert Corporate

You can remove any Acronis Privacy Expert Corporate component separately by selecting **Control panel → Add or remove programs → <The component name> → Remove.** Then follow the instructions on the screen.

Copyright © Acronis, Inc., 2000-2005

Chapter 2. Using Acronis Privacy Expert Corporate Management Console

2.1 Getting started

Acronis Privacy Expert Corporate Management Console is the primary tool for managing Acronis components on remote computers with the Acronis Privacy Expert Corporate Agent installed.

Acronis Privacy Expert Corporate Management Console is launched by selecting **Start → All programs → Acronis → PrivacyExpert → Acronis Privacy Expert Corporate Management Console** or double-clicking the respective desktop shortcut.

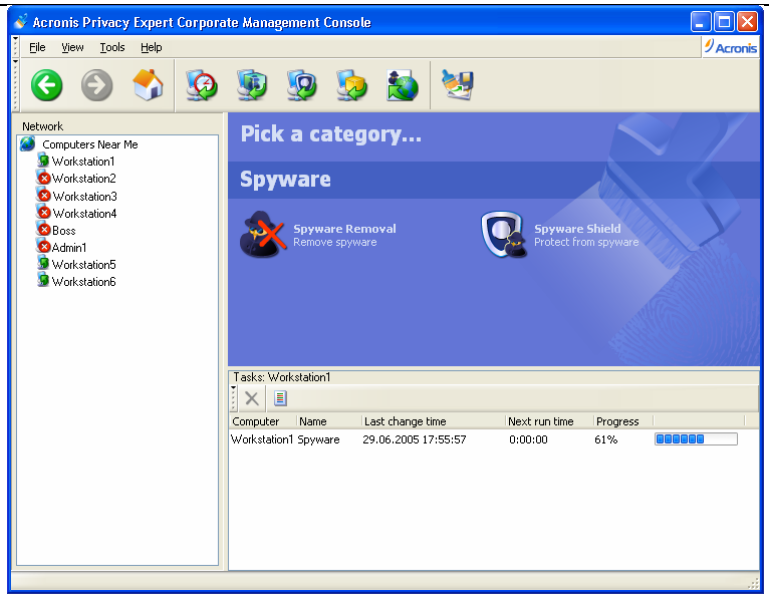
With the Acronis Privacy Expert Corporate Management Console, you can:

- Install Acronis components to remote computers
- Remove spyware and malicious programs from the remote computers (workstations)
- Turn off/on Acronis Spyware Shield on remote computers
- Browse logs of Acronis Privacy Expert Corporate operations
- Browse the remote computers' Quarantines and restore any of deleted objects (files, registry keys etc.), if necessary
- Create bootable media to be able to destroy permanently data on your PC even if it doesn't have Acronis Privacy Expert Corporate installed

2.2 Acronis Privacy Expert Corporate Management Console main window

The Acronis Privacy Expert Corporate Management Console main window contains three areas:

 Copyright © Acronis, Inc., 2000-2005



Acronis Privacy Expert Corporate Management Console main window

- **Operations categories,** where you can select operations to perform on the remote computers (**Spyware Removal** or **Spyware Shield** setting up).

  To move between categories or return to the main window use **Back**, **Next** and **Other categories** buttons on the toolbar.

- **Network** panel contains the list of network computers on which Acronis Privacy Expert Corporate Agent is installed.
- **Tasks** panel displays tasks status for the connected remote computer, selected in the **Network** panel. For the task currently running, a progress bar is displayed. In addition, **Task** panel contains **Show log** button in order to view logs with reports on remote operations for each computer, and **Delete** button to delete scheduled tasks.

2.3 Connecting to remote computer

You need to connect your computer with the management console to the remote computer before you are able to perform any actions with that remote system.

To do so, right-click on the computer name in the **Network** panel and choose **Connect.** In the Remote Connection Wizard window, check the computers you would like to connect.

Then you will be prompted to enter user name and password to access to these computers. It is supposed that accounts with the same username and password exist on all selected computers. Otherwise, you will have to connect to every computer individually.

It is highly recommended that you create an administrator's account with the same username and password on all networked computers for remote access to the Acronis Privacy Expert Corporate Agent.

Copyright © Acronis, Inc., 2000-2005

Chapter 3. Spyware removal from network computers

There are many programs that, once on user's PCs, start working without user's knowledge. Such software can do such things as collect information or change user settings for the Internet or your system. These programs are called **spyware**. For more information on the main spyware types, see **Appendix A** of this guide.

Acronis Privacy Expert Corporate enables you to completely clean user's computers of spyware and protect it from future intrusions.

3.1 How spyware gets on user's PC

One of the most common ways that spyware gets on a user's PC is from new software installations. This is particularly true with freeware and shareware. When user installs such applications, they can implement software modules that collect information on Web sites user visits, user's PC configuration, and other sources

Other common sources of spyware include peer-to-peer networks, gaming portals and other similar Web services.

Sometimes spyware is installed by commercial applications whose makers want to collect additional information about users, their habits and preferences.

3.2 How to recognize spyware?

Though in many cases spyware works without users' knowledge, there are signs that you should watch for:

- Hard drives LEDs are blinking even when no programs are running or documents are open
- User's PC receives and sends unknown information via the Internet, even though the Web browser and e-mail client are not active
- The home page setting of the Internet browser has changed without the user's consent
- The user sees ads or pop-ups while running programs or visiting Web sites

If you notice any or all of these activities on your users' computers, you need to run Acronis Privacy Expert Corporate to find and eliminate spyware performing unauthorized operations on the workstations.

 Copyright © Acronis, Inc., 2000-2005

If you need to:

- Find and remove any type of spyware from remote PCs, run **Spyware removal**
- Prevent spyware from getting on network PCs, enable and set up **Spyware Shield** (see section 4.2 «Spyware Shield local»)

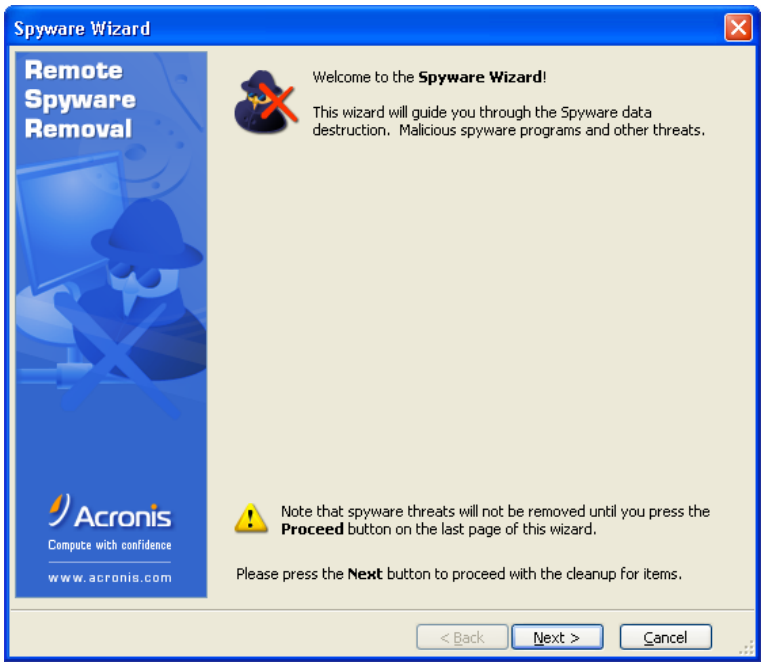
3.3 Spyware removal

Using Acronis Privacy Expert Corporate, you can find and remove spyware from remote computers in your local network. To do this, select and click **Spyware removal** in the main program window.

After that, you can either initiate spyware removal with the **Spyware Removal Wizard** immediately or **update spyware definitions** (see the section Chapter 5 «Spyware» of this guide).

3.3.1 Running Spyware Removal Wizard

To run the **Spyware Removal Wizard,** select **Remove Spyware Now** in the **Spyware Removal** window.

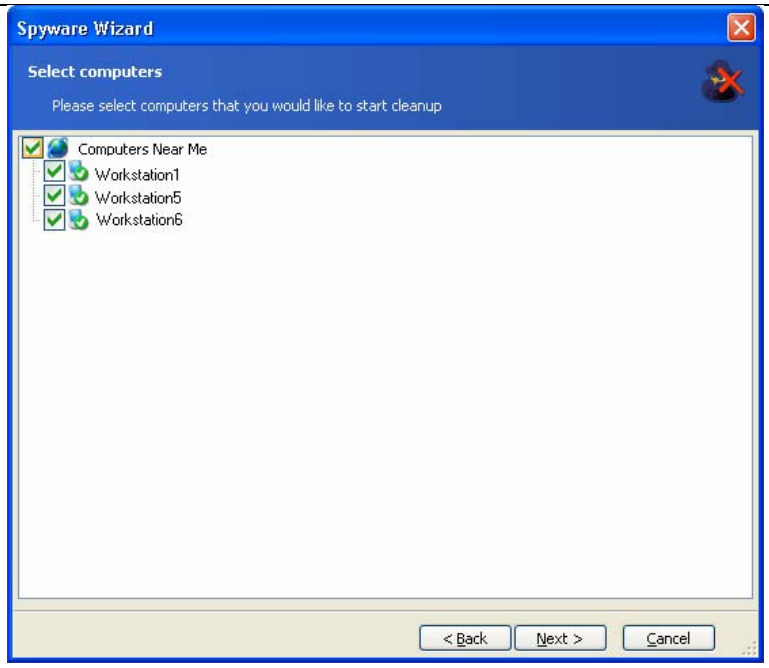

Spyware Wizard
Remote Spyware Removal
Acronis
Compute with confidence
www.acronis.com
Welcome to the Spyware Wizard!
This wizard will guide you through the Spyware data destruction. Malicious spyware programs and other threats.
Note that spyware threats will not be removed until you press the Proceed button on the last page of this wizard.
Please press the Next button to proceed with the cleanup for items.
< Back
Next >
Cancel

Spyware Removal Wizard

3.3.2 Selecting remote computers for spyware removal

In the next window you must select the remote computers on which you are going to remove spyware and malicious programs.

Copyright © Acronis, Inc., 2000-2005

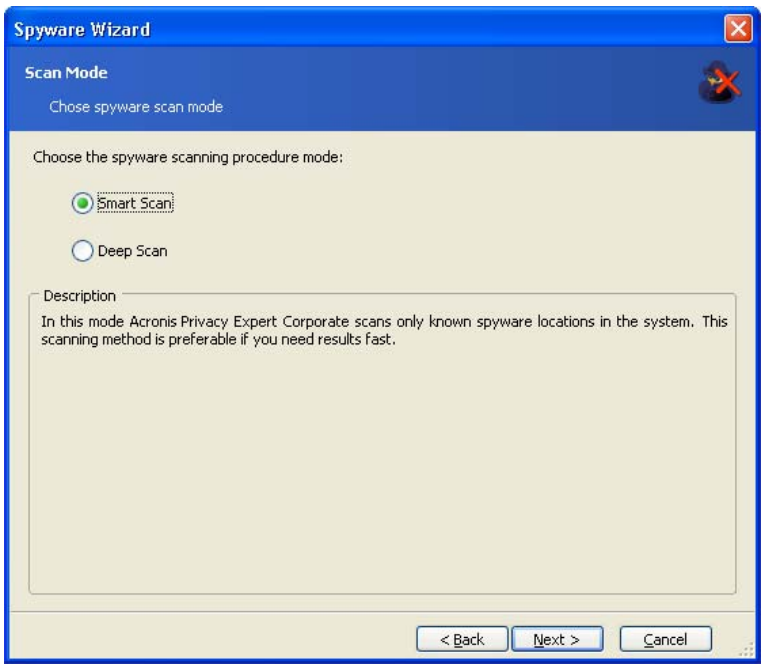


Select computers window

3.3.3 Selecting scanning mode

There are two modes of spyware search:

- **Smart scanning mode** – used by default. The Smart Scanning Mode suite searches for spyware only in the most likely locations, including system, user profile and temporary files folders, as well as in the system registry. Select this mode for a quick PC check.
- **Deep Scanning Mode** – an extended algorithm for spyware scanning. In this mode, all folders on all PC hard drives are searched for spyware. This variant could take much more time depending on the capacity of your hard disks.


Spyware Wizard
Scan Mode
Chose spyware scan mode
Choose the spyware scanning procedure mode:
Smart Scan
Deep Scan
Description
In this mode Acronis Privacy Expert Corporate scans only known spyware locations in the system. This scanning method is preferable if you need results fast.
< Back
Next >
Cancel

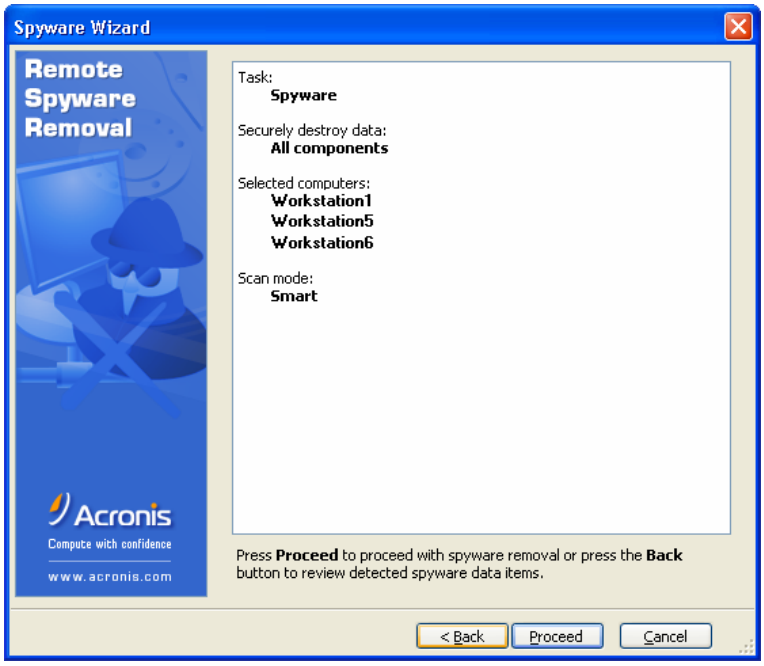
Spyware scanning modes

Copyright © Acronis, Inc., 2000-2005

3.3.4 Spyware Removal Script

In the next window, you will see the final script for the spyware removal operations.

It reports what kinds of spyware are to be removed, a list of remote computers on which this action will be performed, and the spyware scan mode — smart or deep.



Spyware removal operations final script

To execute the script, click **Proceed**.

After the spyware removal operation is finished, you can see logs for each remote computer with a summary that will state the number of spyware applications removed (see section 3.5 «Quarantine»).

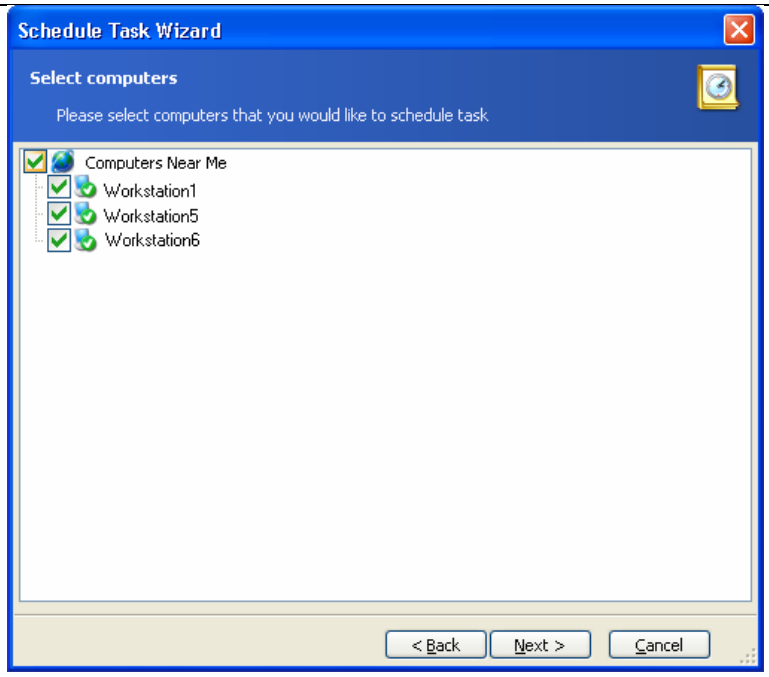
3.4 Scheduling spyware removal group tasks

To set up the removal schedule for remote computers, click the **Schedule task** button on the toolbar of the Acronis Privacy Expert Corporate Management Console main window or select **Tools** → **Schedule task** section in the main menu.

3.4.1 Selecting remote computers

First, select remote computers on which you want to schedule the task.

Copyright © Acronis, Inc., 2000-2005



Select computers window

3.4.2 Selecting task and spyware scan mode

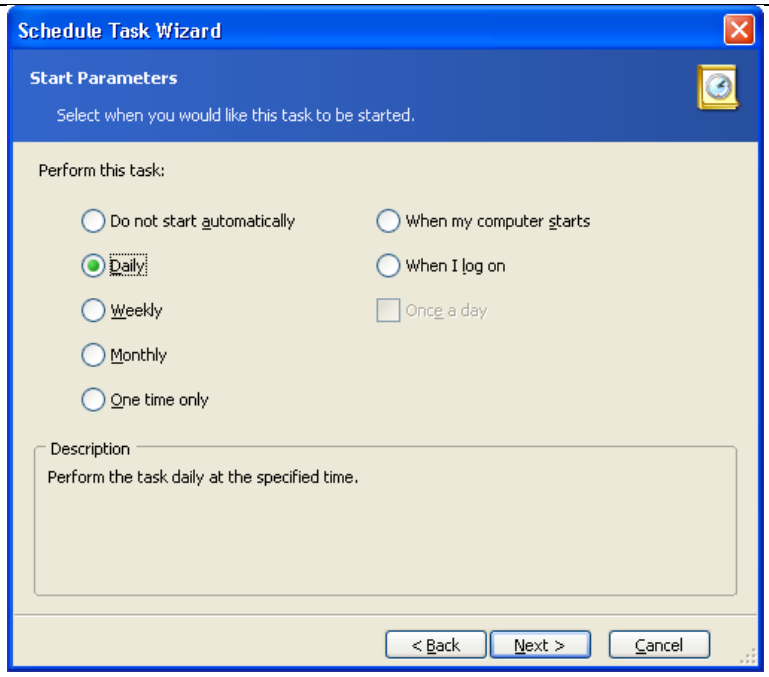
Then you need select the task to schedule (spyware removal) and scan mode (see section 3.3.3 «Selecting scanning mode» of this Guide).

3.4.3 Scheduled tasks preferences

After the remote computers and scan mode are selected you can select the following variants of automatic spyware removal launch:

- **Do not start automatically**
- **Daily**, according to the schedule with the ability to select only workdays or once every few days
- **Weekly**, according to the schedule with the ability to select particular days, such as Tuesday and Friday, or once every two or three weeks, etc
- **Monthly,** according to the schedule on the time and day set; The suite supports clean-up on the <first, second, third, fourth, last> <day of the week> (Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday), for example
- **One time only,** at a specific time (hours:minutes) on a particular day (month/day/year)
- **When my computer starts** (you may specify launching the task once a day only)
- **When I log on** (you may specify launching the task once a day only)

 Copyright © Acronis, Inc., 2000-2005

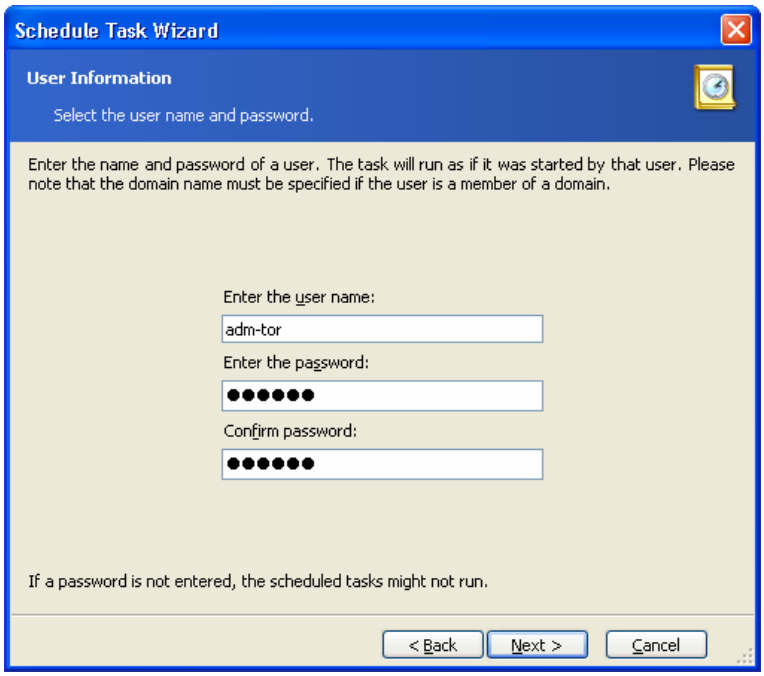


Scheduler set up window

Having made your selection, click **Next** to set additional parameters on the next wizard page.

3.4.4 Entering user name and password

For the remote computers, running Windows NT, 2000, XP or Server 2003, you will have to specify the name of the user that owns the executed task; otherwise, no scheduled execution would be available.


Schedule Task Wizard
User Information
Select the user name and password.
Enter the name and password of a user. The task will run as if it was started by that user. Please note that the domain name must be specified if the user is a member of a domain.
Enter the user name:
adm-tor
Enter the password:
Confirm password:
If a password is not entered, the scheduled tasks might not run.
< Back
Next >
Cancel

In the upper field, enter a user name. Enter a password twice in two fields below. It is supposed that administrator's accounts with the same username and password exist on all selected computers. The task will not start on computers that do not accept the specified user name and password.

You have finished scheduling a task. The wizard will again remind you of the details of the task provided.

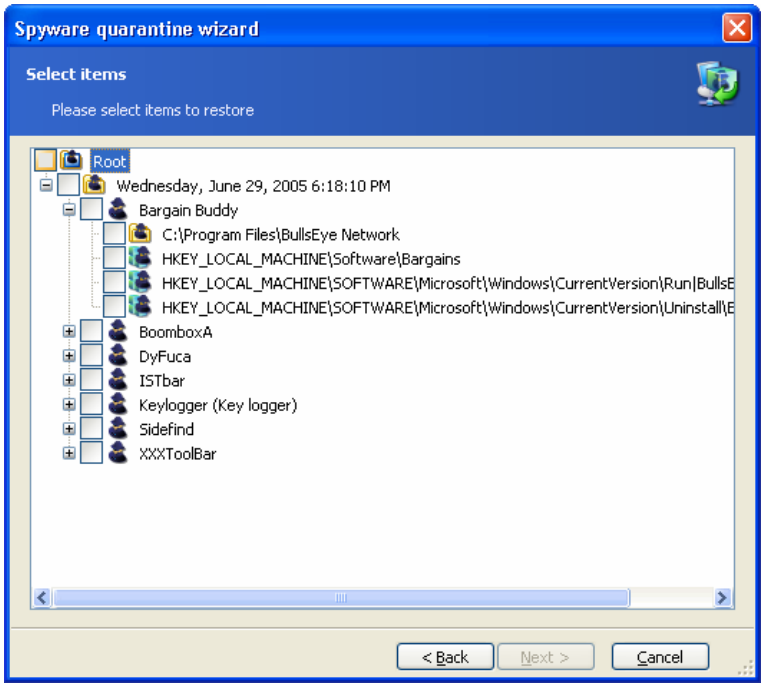
After the task is distributed to selected computers, you can see it in the **Task** panel of the Acronis Privacy Expert Corporate Management Console.

3.5 Quarantine

Though the case is unlikely, you may want to restore some of the items (files, registry keys etc.), deleted by spyware removal operations. Besides, it may be useful to look through the list of deleted objects and obtain the detailed information about Acronis Privacy Expert Corporate operation on remote computers. To allow viewing and recovery of the deleted objects, they are not lost forever, but stored on the user's computer in a special folder, referred to as the Quarantine.

To open the deleted objects list, click the **Spyware Quarantine** button on the Toolbar or select **Tools** → **Spyware Quarantine** from the main menu. Then select a connected remote computer to see its Quarantine. (You can select only one computer at a time. To list other Quarantines, click **Back** after seeing the current one and select the next computer.)

Next, you will see a list of objects, deleted from the selected computer. Now you can check the necessary objects and click **Next** to proceed with their recovery.



Spyware Quarantine list

Copyright © Acronis, Inc., 2000-2005

If the system configuration has been changed since the restored objects were placed to the Quarantine, these objects may be inconsistent with the new system configuration. Therefore, it is recommended that you think twice and use restoration feature in a short time after spyware removal.

The user can empty the Quarantine folder in a usual way, deleting its contents by means of Windows.

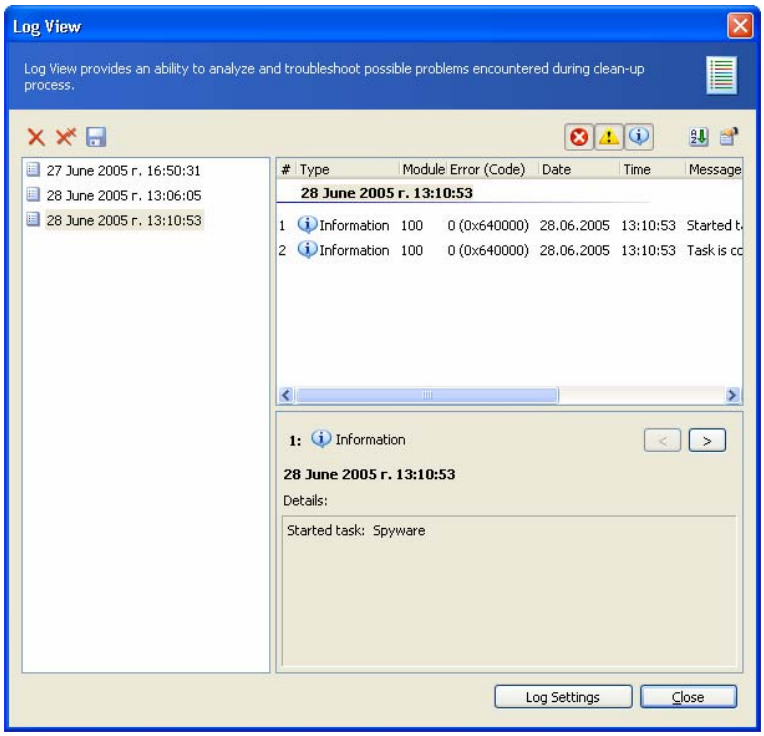
The Quarantine folder address is Documents and Settings/ All Users/ Application Data/ Acronis/ PrivacyExpert8/ SpywareQuarantine. To see this folder, the option **Show Hidden Files and Folders** in **Folder Options** must be enabled.

3.6 Using the Log

The **Log** keeps track of all actions performed by Acronis Privacy Expert Corporate on remote computers. It provides a complete history of activities and reasons for any problems that have occurred.

To view logs:

- Select a computer name from the list in the **Network** panel of the Acronis Privacy Expert Corporate Management Console main window
- Left-click on the **Show log** button in the **Task** panel of the Acronis Privacy Expert Corporate Management Console main window
- You will now see logs for the selected computer.

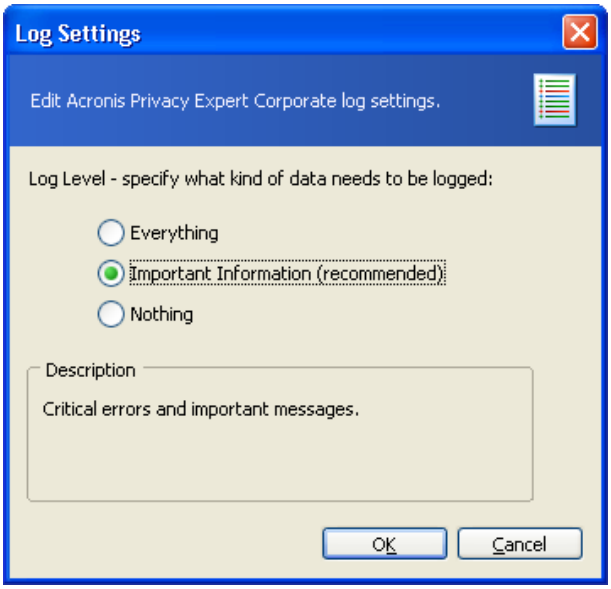

Log View
Log View provides an ability to analyze and troubleshoot possible problems encountered during clean-up process.
27 June 2005 r. 16:50:31
28 June 2005 r. 13:06:05
28 June 2005 r. 13:10:53
Type Module Error (Code) Date Time Message
28 June 2005 r. 13:10:53
1 Information 100 0 (0x640000) 28.06.2005 13:10:53 Started t
2 Information 100 0 (0x640000) 28.06.2005 13:10:53 Task is cc
1: Information
28 June 2005 r. 13:10:53
Details:
Started task: Spyware
Log Settings
Close

Log view window

Copyright © Acronis, Inc., 2000-2005

Log settings enable you to keep track with different degrees of detail. You can select one of the following variants:

- **Everything**
- **Important information** – error and spyware messages
- **Nothing**



Log settings

Copyright © Acronis, Inc., 2000-2005

Chapter 4. Using Acronis Spyware Shield

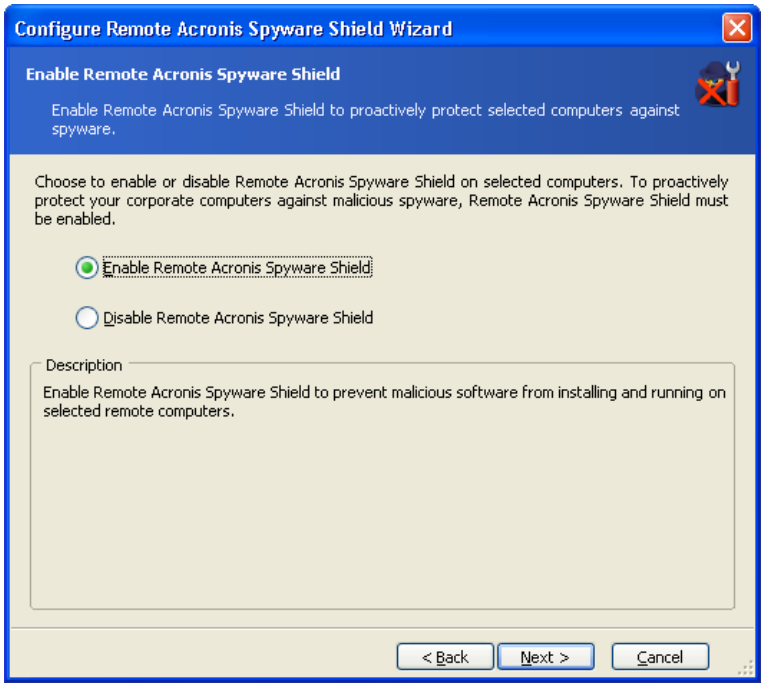
Acronis Privacy Expert Corporate not only enables you to remove spyware from network computers, but it also prevents spyware from accessing the user's PC. This function is provided by the Acronis Spyware Shield — a special tool that monitors computer systems for suspicious applications and components.

4.1 Enabling Acronis Spyware Shield

Spyware Shield comes enable during its remote installation (for more details see Chapter 1 «Installing Acronis Privacy Expert Corporate components»). You can enable or disable it any time you want.

To enable or disable Acronis Spyware Shield on the remote computers:

- select the **Spyware Shield** icon in the Acronis Privacy Expert Corporate Management Console main window or **Configure Spyware Shield** button on the Toolbar
- Run **Configure Remote Acronis Spyware Shield Wizard**
- In the **Select computers** window, select the network computers on which you want to enable or disable the Acronis Spyware Shield
- In the next window, select **Enable** or **Disable** option.


Configure Remote Acronis Spyware Shield Wizard
Enable Remote Acronis Spyware Shield
Enable Remote Acronis Spyware Shield to proactively protect selected computers against spyware.
Choose to enable or disable Remote Acronis Spyware Shield on selected computers. To proactively protect your corporate computers against malicious spyware, Remote Acronis Spyware Shield must be enabled.
Enable Remote Acronis Spyware Shield
Disable Remote Acronis Spyware Shield
Description
Enable Remote Acronis Spyware Shield to prevent malicious software from installing and running on selected remote computers.
< Back
Next >
Cancel

Spyware Shield remote configuration window

To enable or disable Acronis Spyware Shield on the local computer:

Copyright © Acronis, Inc., 2000-2005

- Right-click the **Spyware Shield** icon in the system tray
- Select **Enable Acronis Spyware Shield** or **Disable Acronis Spyware Shield.**

A local computer user can stop the Spyware Shield operation completely (unload the program from the memory) by right-clicking the icon and selecting **Exit**. The Shield icon disappears from the system tray. To start the Spyware Shield again, select **Programs → Acronis → Privacy Expert → Acronis Spyware Shield.**

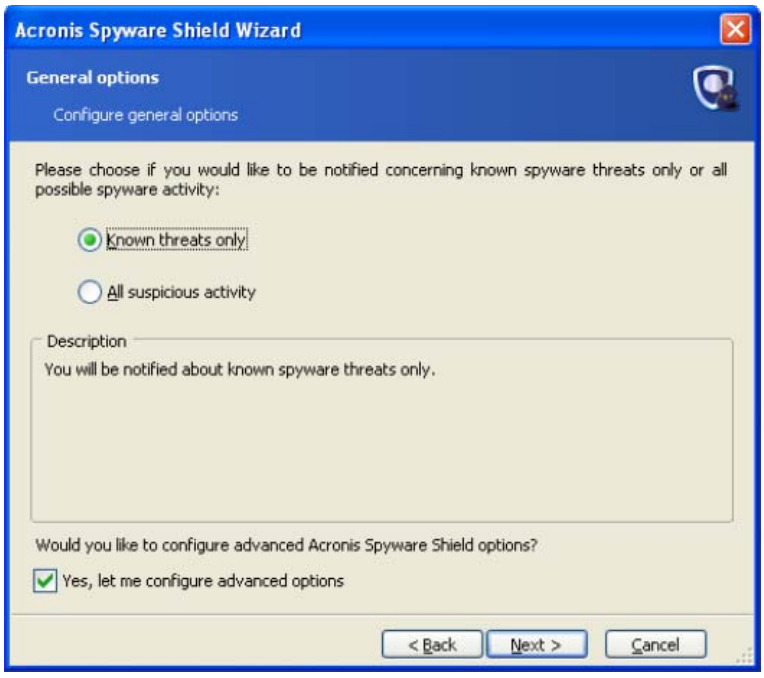
4.2 Spyware Shield local settings

A local computer user can invoke the **Acronis Spyware Shield Wizard** by left-clicking the icon in the system tray. Having enabled **Spyware Shield**, the user can change its settings.

4.2.1 General options

In the **General options** window, you can specify types of spyware from which you want to protect your PC:

- **Known threats only** – **Acronis Spyware Shield** will warn the user only about known spyware activity. This is spyware that is listed in the product's database
- **All suspicious activities – Acronis Spyware Shield** will warn the user about *all* suspicious programs or processes that are trying to change the Windows registry or are launched at startup. This is the recommended setting for experienced users.


Acronis Spyware Shield Wizard
General options
Configure general options
Please choose if you would like to be notified concerning known spyware threats only or all possible spyware activity:
Known threats only
All suspicious activity
Description
You will be notified about known spyware threats only.
Would you like to configure advanced Acronis Spyware Shield options?
Yes, let me configure advanced options
< Back
Next >
Cancel

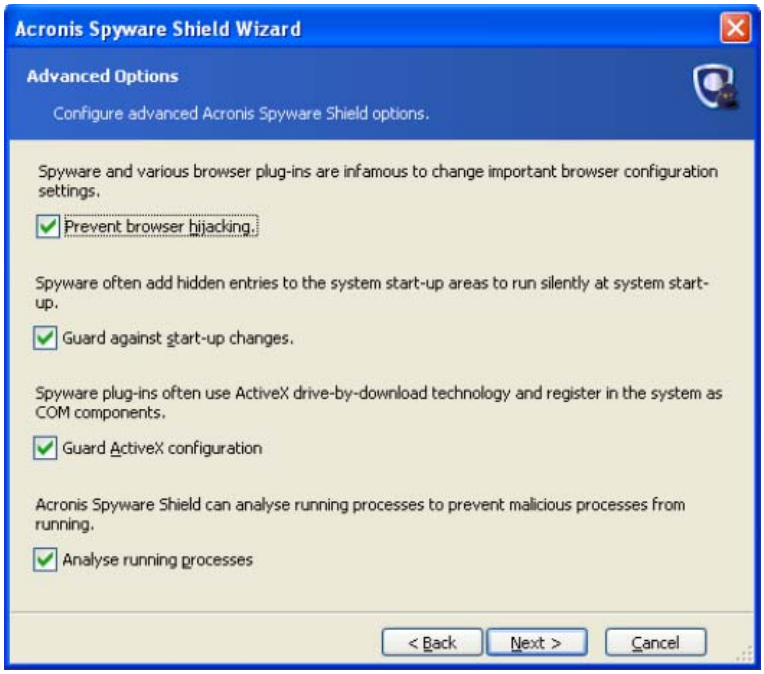
General options window

Copyright © Acronis, Inc., 2000-2005

4.2.2 Advanced options

The **Advanced options** section enables more detailed setup of **Acronis Spyware Shield** and offers the following settings:

- **Prevent browser hijacking** – **Acronis Spyware Shield** will prevent applications from making changes to your Web browser settings, including home page, search page, and more
- **Guard against start-up changes** – will prevent suspicious programs and processes from launching at Windows startup
- **Guard ActiveX configuration** – will prevent changing settings of ActiveX components
- **Analyze running processes** – will constantly monitor running processes and warn you about any suspicious actions of unknown programs


Acronis Spyware Shield Wizard
Advanced Options
Configure advanced Acronis Spyware Shield options.
Spyware and various browser plug-ins are infamous to change important browser configuration settings.
Prevent browser hijacking.
Spyware often add hidden entries to the system start-up areas to run silently at system start-up.
Guard against start-up changes.
Spyware plug-ins often use ActiveX drive-by-download technology and register in the system as COM components.
Guard ActiveX configuration
Acronis Spyware Shield can analyse running processes to prevent malicious processes from running.
Analyse running processes
< Back
Next >
Cancel

Advanced options window

4.2.3 Remembered events

While **Spyware Shield** running, it alerts you on suspicious software activity by showing dialog boxes, containing the detected process essence and two buttons for you to enter your decision. Choose **Block** if you want to prevent the action, or **Allow** to allow the change to be applied to the system. If you want to permanently block or allow that action, check **Remember event** box. The shield will not alert you on the remembered action any more, unless you uncheck the action in **Remembered events** window.

Copyright © Acronis, Inc., 2000-2005

4.2.4 Saving Spyware Shield settings

Having set up **Spyware Shield**, you can browse the resulting settings in the final script and click **Apply** if everything is correct.

All **Spyware Shield** settings will be active until you change them again.

Copyright © Acronis, Inc., 2000-2005

Chapter 5. Spyware definitions updates

Offering you timely and reliable protection from new spyware released as often as every day, Acronis Privacy Expert Corporate launches the special **Spyware definitions updates** service. It enables users to obtain the most up-to-date information and spyware protection from Acronis website.

5.1 Product registration

Remember that the Spyware definitions updates service is available *only* for registered users of Acronis Privacy Expert Corporate.

You can register you copy of the program at the Acronis here:

http://www.acronis.com/enterprise/registration/

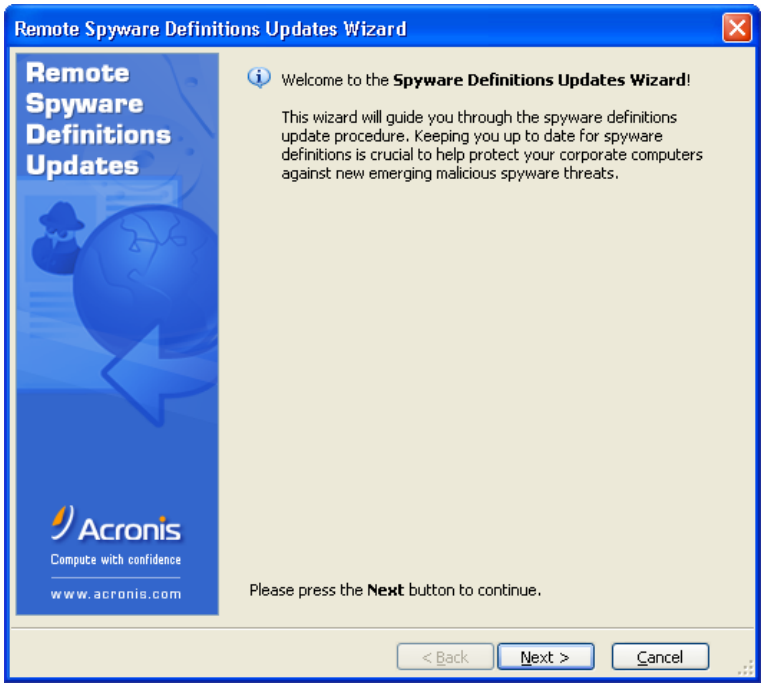
Your login is your valid email address.

5.2 Spyware database update

5.2.1 Running Spyware Definitions Updates Wizard

You can run the **Spyware Definitions Updates Wizard** in the Acronis Privacy Expert Corporate Management Console main window the following ways:

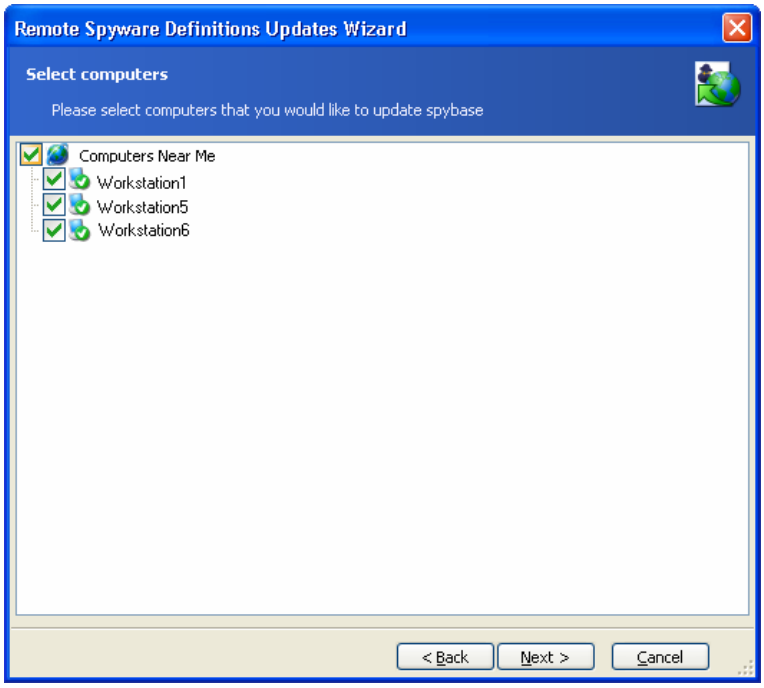
- By selecting **Tools** → **Web updates** in the menu
- By clicking **Web updates** on the toolbar.


Remote Spyware Definitions Updates Wizard
Remote Spyware Definitions Updates
Welcome to the Spyware Definitions Updates Wizard!
This wizard will guide you through the spyware definitions update procedure. Keeping you up to date for spyware definitions is crucial to help protect your corporate computers against new emerging malicious spyware threats.
Acronis
Compute with confidence
www.acronis.com
Please press the Next button to continue.
< Back
Next >
Cancel

Spyware definitions update wizard

5.2.2 Selecting remote computers to update spyware definitions

Next, select the remote computers on which you are going to update spyware definitions.



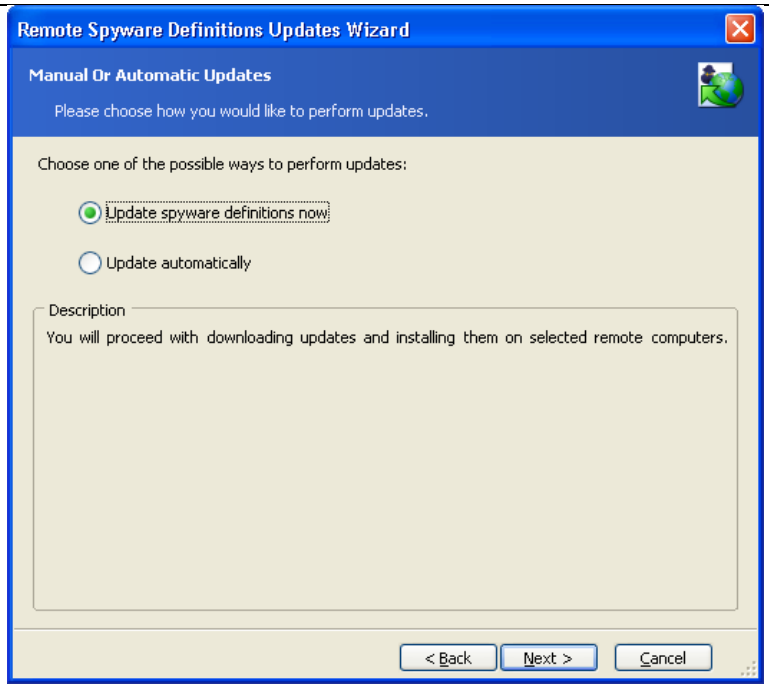
Select computers window

5.2.3 Selecting update mode

Having run the **Spyware Definitions Updates Wizard**, you can select the update mode: either manual or scheduled automatic:

- To update spyware definitions **right now**, select **Update spyware definitions now**
- To **automatically update** spyware definitions on a schedule, select **Update automatically**.

Copyright © Acronis, Inc., 2000-2005


Remote Spyware Definitions Updates Wizard
Manual Or Automatic Updates
Please choose how you would like to perform updates.
Choose one of the possible ways to perform updates:
Update spyware definitions now
Update automatically
Description
You will proceed with downloading updates and installing them on selected remote computers.
< Back
Next >
Cancel

Selecting update mode window

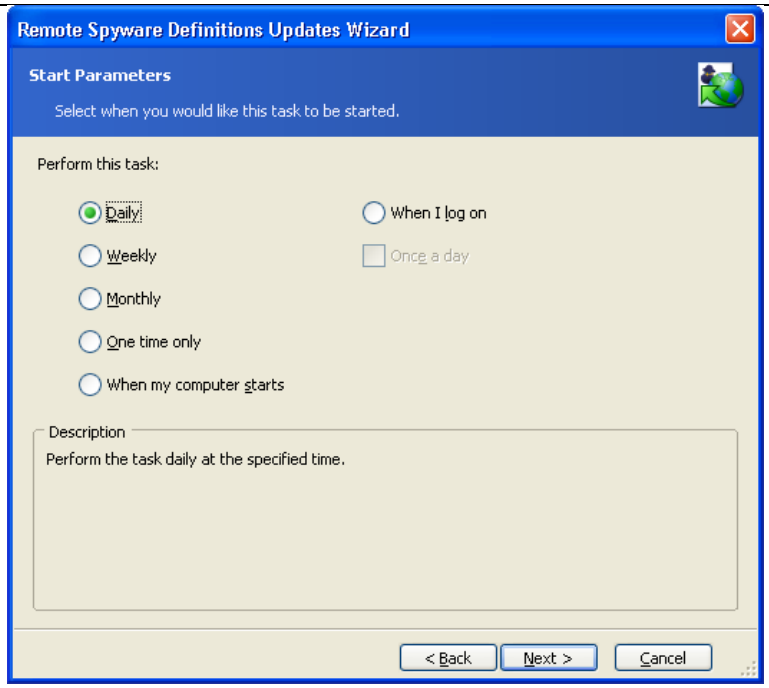
5.2.4 Setting the schedule

If you select automatic updates, you will be asked to set the update schedule.

The following variants are available:

- **Daily**, according to the schedule with the ability to select only workdays or once every few days
- **Weekly**, according to the schedule with the ability to select particular days, such as Tuesday and Friday, or once every two or three weeks, etc
- **Monthly,** according to the schedule on the time and day set; The suite supports clean-up on the <first, second, third, fourth, last> <day of the week> (Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday), for example
- **One time only,** at a specific time (hours:minutes) on a particular day (month/day/year)
- **When my computer starts** (you may specify launching the task once a day only)
- **When I log on** (you may specify launching the task once a day only)

Copyright © Acronis, Inc., 2000-2005



Set the update schedule

Having made a selection, click **Next** to set additional parameters on the next wizard page.

5.2.5 Entering user name and password

To finish scheduling automatic updates, enter the user name and password for access to the remote computers. See details in 3.4.4.

Copyright © Acronis, Inc., 2000-2005

Chapter 6. Acronis Pop-up Blocker

6.1 What are pop-ups?

While browsing some Web sites, you might have unwanted pop-up windows open along with the window you want. Generally, pop-ups contain bothersome advertising. They slow down your Internet connection and increase the traffic you pay for. On some Web sites, pop-ups are used to provide extra information or as locations where the user needs to input information.

6.2 Acronis Pop-up Blocker

Acronis Pop-up Blocker automatically prevents windows from opening, except the ones the user wants to view.

You can install Acronis Pop-up Blocker remotely using the Acronis Privacy Expert Corporate Management Console (See section 1.8 «Installing Acronis components onto remote machines» of this Guide).

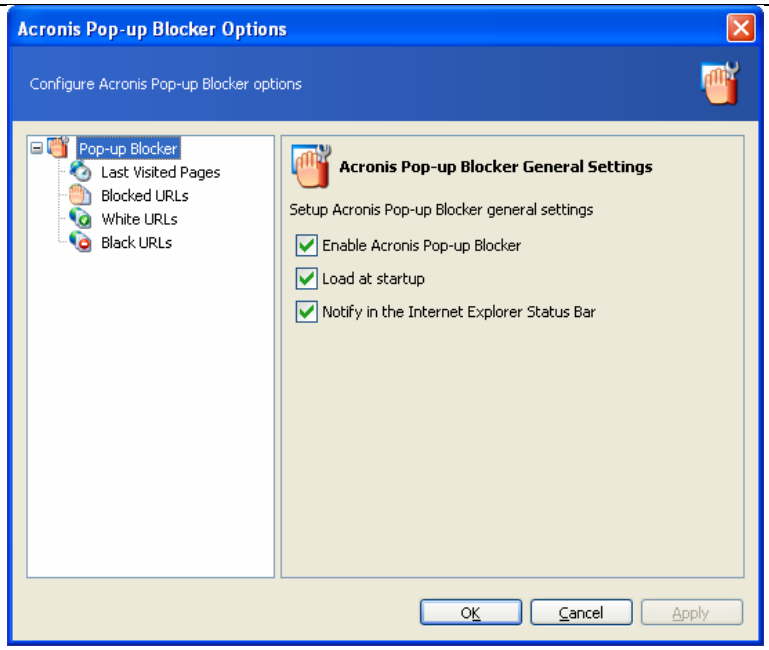
After that, the local user can disable/enable the Acronis Pop-up Blocker or change its options by right-clicking the icon in the system tray and selecting the item from the context menu.

A local computer user can stop the Acronis Pop-up Blocker operation completely (unload the program from the memory) by right-clicking the icon and selecting **Exit**. The Pop-up Blocker icon disappears from the system tray. To start the program again, select **Programs → Acronis → Privacy Expert → Acronis Pop-up Blocker**.

6.3 Acronis Pop-up Blocker local options

A local user can invoke the Acronis Pop-up Blocker options window by double-clicking the Pop-up Blocker **icon** in the system tray with the left mouse button.

Copyright © Acronis, Inc., 2000-2005



Pop-up Blocker settings

6.3.1 Acronis Pop-up Blocker general settings

In the general settings section, you can enable or disable the following:

- Enable Acronis Pop-up Blocker
- Load it at startup
- Check on its status in the IE status bar

6.3.2 Last visited pages

The **Last visited pages** section is a duplicate of the **Microsoft Internet Explorer History.**

In this list, you can select Web sites to add to either the White or the Black list.

6.3.3 Blocked URLs

In this section, you can see which Web sites contained pop-ups that were blocked.

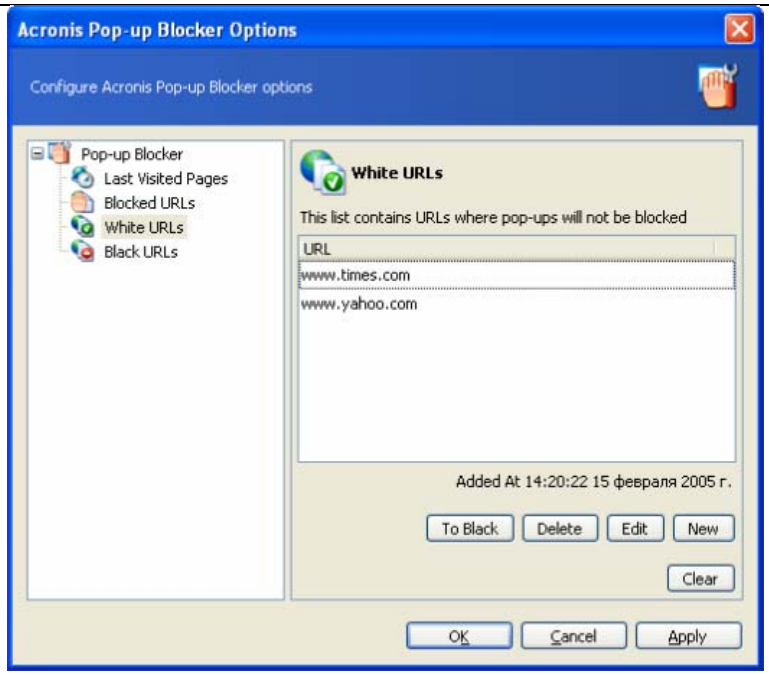
You can add any of these to either the White or the Black list.

6.3.4 White URLs

If you want to cancel the Acronis Pop-up Blocker for a particular Web site, you can move it to the White (approved) list:

- By clicking "New" and entering it manually
- By selecting the address and clicking **To White** in the **Last visited pages, Blocked URLs**, or **Black list** windows.

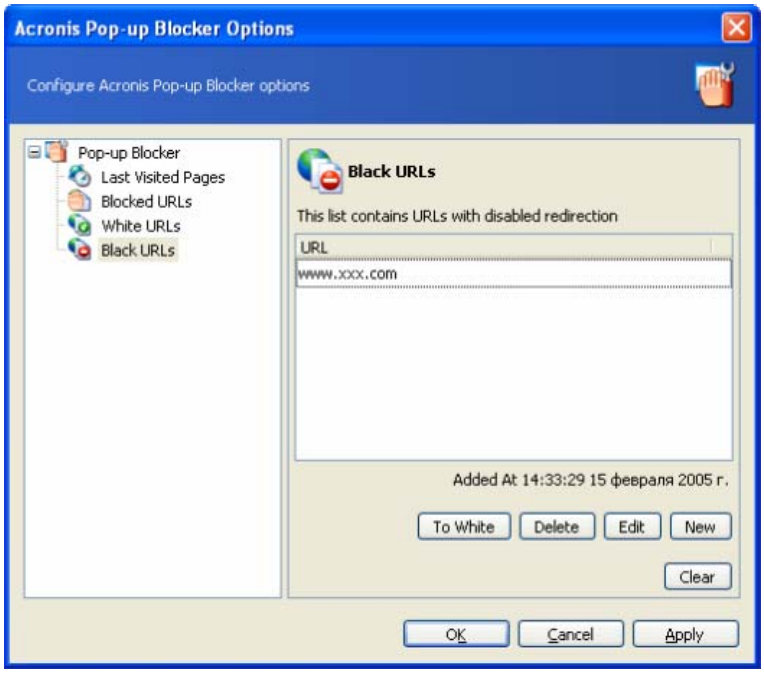
Copyright © Acronis, Inc., 2000-2005



White list window

6.3.5 Black URLs

Adding the site to the Black (rejected) list means that Acronis Pop-up Blocker will prevent you from following any link, available on this site, and show a report in IE bar (if enabled): "Acronis Pop-up Blocker: Black URL link – navigation stopped".



Black list window

Copyright © Acronis, Inc., 2000-2005

Chapter 7. Other operations

7.1 Creating a bootable diskette or CD with Acronis Drive Cleanser

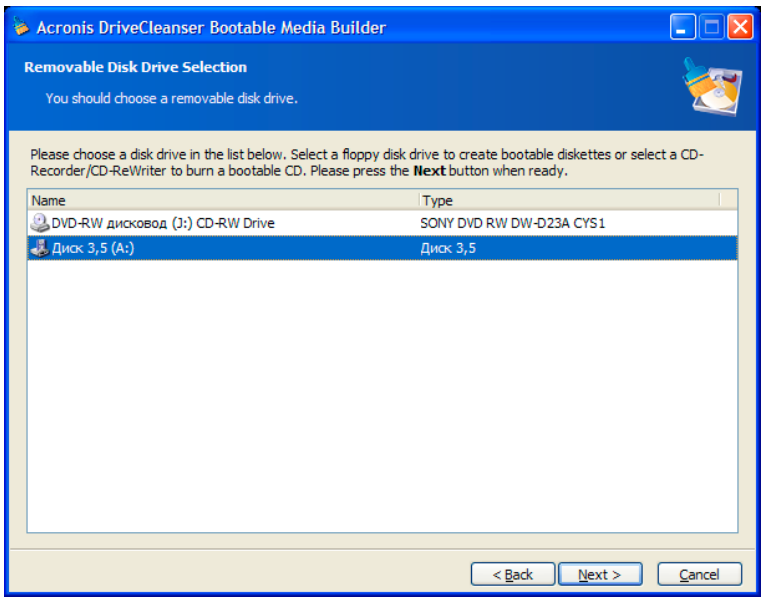
Many operating systems do not provide users with sufficient data destruction tools, so deleted files can be restored easily by simple applications. Even a complete disk reformat cannot guarantee permanent confidential data destruction.

Acronis Drive Cleanser solves this problem with guaranteed and permanent data destruction on selected hard disks and/or partitions. It allows you to select from a number of data destruction methods depending on the importance of your confidential information.

Using the Acronis Privacy Expert Corporate, you can create a bootable diskette or CD with Acronis Drive Cleanser.

This diskette or CD will allow you to destroy data on your PC easily and permanently, even if it doesn't have Acronis Privacy Expert Corporate installed.

To create a bootable diskette, select **Bootable Media Builder** button in the **Toolbar** and follow the **wizard** instructions.


Acronis DriveCleanser Bootable Media Builder
Removable Disk Drive Selection
You should choose a removable disk drive.
Please choose a disk drive in the list below. Select a floppy disk drive to create bootable diskettes or select a CD-Recorder/CD-ReWriter to burn a bootable CD. Please press the Next button when ready.
Name
Type
DVD-RW дисковод (J:) CD-RW Drive
SONY DVD RW DW-D23A CYS1
Диск 3,5 (A:)
Диск 3,5
< Back
Next >
Cancel

Selecting media

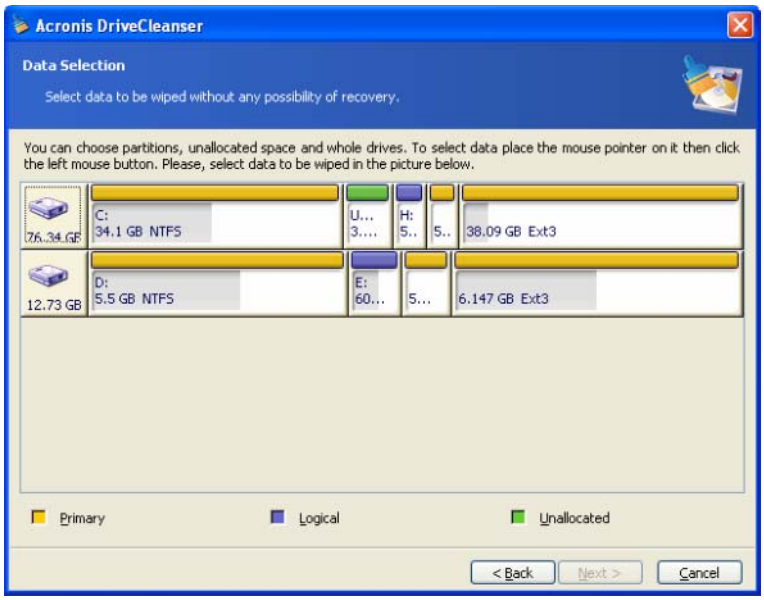
7.2 Data destruction with Acronis Drive Cleanser

Acronis Drive Cleanser is based on a **wizard** that **scripts** all hard disk operations, so no data destruction is performed until you execute the complete script. At any

Copyright © Acronis, Inc., 2000-2005

stage, you can return to the previous stages to select other disks, partitions or data destruction methods.

- Insert the boot disk into the disk drive and boot from that disk (change the order of boot devices in BIOS, if necessary).
- To select a disk/partition, where you want to destroy data, click the corresponding rectangle. A red mark in the upper right corner appears, indicating that the disk/partition is selected. You can select any combination of disks/partitions.


Acronis DriveCleanser
Data Selection
Select data to be wiped without any possibility of recovery.
You can choose partitions, unallocated space and whole drives. To select data place the mouse pointer on it then click the left mouse button. Please, select data to be wiped in the picture below.
C:
34.1 GB NTFS
38.09 GB Ext3
D:
5.5 GB NTFS
6.147 GB Ext3
12.73 GB
Primary
Logical
Unallocated
< Back
Next >
Cancel

The list of PC hard disks with partitions

- Next, select a data destruction method. Acronis Drive Cleanser utilizes a number of the most popular data destruction methods, complying with national standards including U.S. Standard DoD 5220.22-M. You may create your own method in further wizard windows as well, or load a method from an *.alg file.
- In the next window, check carefully the final script of operations. After you click **Proceed**, Acronis Drive Cleanser will start wiping the disk, indicating the progress in the special window.
- After the procedure is finished, you can estimate its result by reading and displaying the data from the wiped disk/partition, using Acronis Disk Editor tool. The picture you might see depends on the data destruction method. But what you actually see are disk sectors filled with either zeros or random symbols.

Copyright © Acronis, Inc., 2000-2005

Appendix A. Spyware threats glossary

This glossary contains supplemental information on the most popular spyware from which Acronis Privacy Expert Corporate protects your organization computers.

Adware

This is a kind of Web marketing where banners are integrated into freeware and shareware programs. To be able to use a program, a user has to watch ads downloaded from the Web. This increases traffic volume and slows down your Internet connection.

Browser Helper Objects

Some Browser Helper Objects are useful at expanding your browser's capabilities, but there are others that might not need your permission to install on your computer and that can be used for malicious purposes, such as gathering information on your Web surfing habits. This can cause problems ranging from incompatibility issues to corrupting important system functions, making these objects not only a threat to your security, but also to your system's stability.

Browser hijackers

Browser hijackers have the ability to change your Internet browser settings, redirect your Web searches through their own search engines, redirect mistyped or incomplete URLs, and change your default home page. They can redirect your searches to "pay-per-search" Web sites or pornographic Web sites.

Commercial keylogger

Keyloggers register which keys are pressed on a user's PC and transmit this information via e-mail. Such applications can also store the time of running or quitting any applications. They can operate without the users' knowledge.

Dialers

Dialers have the ability to disconnect your computer from your local Internet provider and reconnect you to the Internet using an alternate connection, such as an expensive pornographic, toll or international phone number. They do not spy on you but they can rack up significant long-distance phone charges. They have the ability to run in the background, hiding their presence.

Copyright © Acronis, Inc., 2000-2005

Exploit/Security holes

These are security bugs and vulnerabilities in applications primarily meant for Web operations. Through such holes, intruders can corrupt a PC or gain remote control over it.

Remote Administration

This is a kind of software, including commercial software, designed for remote PC control. In some cases, users might not be aware of such applications running.

Sniffers

Sniffers are programs that capture network traffic (sent and received data packets). Sniffers can be a serious threat, able to capture and decrypt user names, passwords and private information and prevent normal operation of computers and networks in general. As most protocols (FTP, POP, HTTP, telnet) have secret information transmitted unencrypted, an intruder can easily gain access to a user's information by setting up sniffer filters and waiting for the victim to connect to a server.

Spyware

Spyware are programs that secretly gather and transmit personal user information. Spyware can be a part of various applications, including commercial products.

Toolbars

Toolbars can be downloaded to your Web browser to make browsing easier. Examples include the Google, Alexa and Yahoo toolbars. Even though these are very handy to use, they have the ability to track everything you do on the Internet and to pass that information back to the owners of the toolbars. Be sure to read the terms and conditions page before you download any toolbar.

Trojan Horses (Trojans)

Trojans are specially created programs that are deployed to PCs imitating useful applications and utilities. They can result in failures, lock-ups or even complete data destruction. Trojans are spread via mailing lists, Web forums, etc.

Copyright © Acronis, Inc., 2000-2005